

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF GEORGIA
SAVANNAH DIVISION

UNITED STATES OF AMERICA)
)
v.) Case No. CR413-007
)
LEROY CHISOLM, VINCENT)
BRYANT, and RICARDO CRAWFORD)

REPORT AND RECOMMENDATION

Three of the twenty-three defendants charged as coconspirators in this drug case have moved to suppress the evidence secured by the investigators through court-authorized wiretaps of various cellular telephones.¹ Vincent Bryant challenges only the “necessity” for the wiretap under 18 U.S.C. § 2518(1)(c). In addition to that argument, defendants Leroy Chisolm and Ricardo Crawford also contend that the

¹ Not one of the three defendants filed his own, separate motion to suppress the wiretaps but instead simply adopted a suppression motion filed by another defendant in the case. As reflected by the Notices to Counsel returned by these defendants (which the clerk is directed to make a part of the record), defendants Leroy Chisolm and Ricardo Crawford both adopt the suppression motion filed by defendant Grilly Holloway, doc. 217 (which Holloway has since withdrawn). Defendant Vincent Bryant has adopted the suppression motion filed by codefendant Chad McCoy, doc. 200 (since withdrawn by McCoy).

wiretap fails for lack of probable cause, failure to minimize communications not subject to interception, improper sealing of the seized conversations (an argument adopted by Bryant at the suppression hearing), improper seizure of geolocation data, and failure to specify the persons whose communications are to be intercepted, the description of those communications, the location of the listening post, and the law enforcement agency that would conduct the intercepts. Doc. 217. None of these challenges to the validity of the wiretaps withstands scrutiny.

I. BACKGROUND

Starting in December 2011 and continuing through November 2012, state and federal investigators sought and obtained a series of orders² authorizing the use of wiretaps on numerous cellular telephones utilized by various individuals known to be engaged in a drug conspiracy. All three defendants were captured on Target Telephone (“TT”) 1.³ As the wiretap affidavits for TT 1-10 make the same basic showing, it is clear that if the application and authorization for TT 1 is defective, then

² There were a total of 16 wiretap authorizations. Gov’t ex. 1.

³ Defendant Chisolm was also intercepted on TT 2-5 and 7-10, defendant Bryant was intercepted on TT 2-4 and 7-9, and defendant Crawford was intercepted on TT 9. It is undisputed that each defendant is an “aggrieved person” who has standing to challenge any wiretap which resulted in the interception of his own communications. 18 U.S.C. §§ 2510 (11), 2518 (10)(a).

all subsequent wiretap applications and orders applicable to these defendants are similarly defective and, conversely, that if the initial wiretap authorization and order are valid, then the later wiretaps are likewise valid.

On December 14, 2011, Chatham County Superior Court Judge Louisa Abbot authorized the wiretap of two cellular telephones used by Anthony King.⁴ The wiretap application for Target Telephones (“TT”) 1 and 2 was supported by a 94-page affidavit from state narcotics agent David Arbizo. TT 1 aff. That affidavit recounted in great detail the long and complex history of law enforcement efforts to investigate the drug trafficking activities of King, Elmore Michael Singleton, and some of their associates. King’s name (and Singleton’s) had surfaced in 2006 during the investigation and successful prosecution of a multi-defendant drug organization headed by Kobie Ervin. *Id.* at 10-12.⁵ During a 2008

⁴ The wiretap affidavit states that Anthony King had used numerous aliases, including “GEZ” and “Ghost.” TT 1 aff. At 1. King is charged in the present indictment as “Jarvis King.” Doc. 1.

⁵ That investigation, which also involved the use of a wiretap, abruptly ended when intercepted calls revealed that Ervin and his father had kidnapped and were about to murder two individuals. TT 1 aff. at 11. The premature interruption of the investigation thwarted the investigator’s efforts to identify Ervin’s suppliers. *Id.* During a later debriefing following his conviction, Ervin told agents that King and Singleton were his cocaine suppliers. *Id.* at 14.

investigation of Pascal Green, another drug trafficker, agents gained wiretap evidence that King was Green's source of supply and that King had his own source of supply in Atlanta, Georgia. *Id.* at 13. Agents then obtained authorization to wiretap King's phone, but a state judge later suppressed all evidence obtained pursuant to that wiretap.⁶ *Id.*

In 2011, both the Chatham Savannah Counter Narcotics Team ("CNT") and the DEA launched a new investigation of King. By devoting considerable law enforcement resources and time to this endeavor, agents were able to amass a wealth of information from confidential informants, surveillance, and toll records analysis about the membership and structure of the drug organization. *Id.* at 18-19. Agents then made controlled purchases of drugs from one of King's main distributors in South Carolina. *Id.* at 19. A CNT informant related that in December 2003 King had traveled to El Paso, Texas to meet with a Mexican source of cocaine and marijuana. *Id.* at 19-20. A DEA

⁶ The affiant for the present wiretap affidavit emphasized "**that all information in [his] affidavit was obtained independent of the suppressed wiretap.**" TT 1 aff. at 13 (emphasis in original). None of the motions to suppress presently before the Court challenge this representation. While defendant Bryant's attorney endeavored to raise the issue at the suppression hearing, he proffered no evidence that called into question the validity of the affiant's assertion.

informant stated that during 2004 and 2005 he had regularly purchased one-quarter kilogram quantities of cocaine from King and that he had observed King in the possession of over 100 pounds of marijuana and some 5 to 10 pounds cocaine. *Id.* at 21-22.

In February 2011 the DEA arranged to have its informant reestablish contact with King and Singleton. *Id.* at 23. Through surveillance and monitoring phone calls between the informant and King, agents confirmed that King was still trafficking in drugs and that he took elaborate measures to avoid law enforcement detection of his activities. *Id.* King frequently changed cellular telephones and cautioned the informant that he must do likewise, and that he should avoid driving flashy cars. *Id.* at 22-30, 39.

On two occasions in June 2011, agents succeeded in having the informant make two controlled purchases of cocaine from King. *Id.* at 34-36.⁷ In October 2011, agents had the informant make a third controlled purchase of cocaine from King, and they also surveilled the informant as he either met with King personally or spoke with him by

⁷ In July 2011, during an unrelated investigation of another drug dealer not known to have any ties with King, agents discovered substantial links between that dealer and the King organization. TT 1 aff. at 37-38.

phone (on TT 1) to negotiate other drug transactions. *Id.* at 38-58. Agents had their informant make yet another controlled purchase of cocaine from King in November 2011. *Id.* at 58-59. King called the informant on TT 2 -- his *tenth* cellular phone in as many months -- a few days later. *Id.* at 63. Through pen register and toll record analysis, agents identified numerous individuals with whom King had frequent contact. *Id.* at 62-71. Many of these individuals were known by the agents to be in the drug trade. *Id.* at 5-9, 62-71.

Agent Arbizo explained in his affidavit that the goal of the investigation was not simply to arrest the known targets or seize a single storehouse of narcotics, but rather to “disable and dismantle the vertical distribution network of narcotics that extends around the target individual(s), both to subsidiary dealers who obtain narcotics from them, as well as those who supply narcotics to them.” *Id.* at 71, 74 (noting that King was but “a part” of the narcotic distribution network and that the goal of the investigation was to arrest and convict not only King and Singleton but also “their co-conspirators, and others yet unknown”). Arbizo stated that while the agents had identified numerous individuals by name, including targets in other states, the investigation had failed to

establish sufficient evidence to conduct a successful prosecution of those individuals. Arbizo further explained that neither the use of physical surveillance (including a pole camera) nor confidential informants (who remained on the fringe of the organization) had succeeded in achieving these objectives, and he noted that the use of other investigative techniques (such as undercover agents, interviews, grand jury subpoenas, and search warrants) would likely compromise the investigation and pose a potential threat to informants. *Id.* at 74-85.

On the strength of this elaborate showing of probable cause and necessity, Superior Court Judge Abbot approved the use of the wiretap on target phones 1 and 2. Subsequent wiretap authorizations by both state and federal court judges, while supplemented by additional information, rested upon the same basic showing.

II. ANALYSIS

A. Probable Cause

Two defendants (Chisolm and Crawford) make the unsupported allegation that the affidavit failed to establish even probable cause to believe that the target telephones would be used in furtherance of any criminal activity. Doc. 217 at 6-7. But as the above summary of the

affidavit reflects, the agents established conclusively that King was a major drug dealer who regularly used his cellular telephones as part of his drug business. Not only that, the affidavit reflected King's use of both TT 1 and TT 2 for that very purpose. *Id.* at 58, 60, 68-70. The probable cause basis for the wiretap is not debatable.

B. Necessity

All three defendants allege that the government failed to satisfy the "necessity" requirement of 18 U.S.C. § 2518(1)(c), which demands that each wiretap application reflect that "other investigative procedures have been tried and failed or . . . reasonably appear unlikely to succeed if tried or to be too dangerous." *Id.* Defendants point to the mountain of evidence already secured by the investigators using traditional investigative techniques, but nowhere do they mention or endeavor to counter the affidavit's statement that these investigative techniques had proven unsuccessful in accomplishing the goal of identifying all the members of the conspiracy, the drug network's sources of supply and transportation methods, or the location of narcotics caches and illicit proceeds of the drug enterprise. Rather, defendants assert that the government should have continued to pursue their investigation utilizing

the same methods already employed, as well as certain additional investigative techniques that had yet to be tried. Doc. 200 at 7; doc. 217 at 8.

The burden of establishing necessity is “not great.” *United States v. Acosta*, 807 F. Supp. 2d 1154, 1239 (N.D. Ga. 2011) (quoting and citing *United States v. Gray*, 410 F.3d 338, 343 (7th Cir. 2005)). “The necessity requirement is designed to ensure that electronic surveillance is neither routinely employed nor used when less intrusive techniques will succeed. . . . The affidavit need not, however, show a comprehensive exhaustion of all possible techniques, but must simply explain the retroactive or prospective failure of several investigative techniques that reasonably suggest themselves.” *United States v. Van Horn*, 789 F.2d 1492, 1495-96 (11th Cir. 1986). The government’s showing of necessity “must be read in a ‘practical and commonsense fashion,’” and the district court is entitled to “broad discretion” in making its assessment of necessity. *United States v. Alonso*, 740 F.2d 862, 868 (11th Cir. 1984). An order authorizing a wiretap “will not be overturned ‘simply because defense lawyers are able to suggest *post factum* some investigative

technique that might have been used and was not.”” *Id.* at 869 (quoting *United States v. Hyde*, 574 F.2d 856, 867 (5th Cir. 1978)).

As the affidavit makes clear, while the agents had amassed considerable evidence against King -- evidence sufficient to prosecute him for several drug transactions involving relatively small amounts of cocaine (1/2 to 2 ounce quantities) -- they had been unable to develop information about the full scope of his King’s own activities (for a few hand-to-hand drug sales were “hardly representative of King’s level of involvement in the criminal enterprise”), much less gather beyond-a-reasonable-doubt proof as to all other members of the conspiracy. TT 1 at 74-75. King was quite knowledgeable about law enforcement investigative techniques, and he regularly engaged in counter-surveillance methods that made additional surveillance unlikely to reap more than “ancillary dividends.” *Id.* at 60, 75 (noting that despite law enforcement interest in King for “11 years,” the agents had been unable to penetrate deeply into his organization or develop sufficient evidence of the full range of its criminal activities and membership essential to a successful prosecution). The informants were of limited utility, as they remained on the periphery of the organization, *id.* at 79, a pole camera

installed by the agents had to be removed because a person under observation became too curious about the device, *id.* at 78, additional controlled purchases from King would not expand the agents' knowledge of the conspiracy's much larger scope, *id.* at 80-81, and the further examination of toll records offered little hope of unraveling the organization's complex structure. *Id.* at 85-86. Finally, the use of additional techniques, such as search warrants, grand jury subpoenas, trash pulls, etc., were more likely to compromise rather than further the investigation.

Because the agents' use of conventional investigative techniques (those reasonably appropriate under the circumstances) had failed to furnish sufficient evidence to dismantle the drug organization and successfully prosecute each of its members, it was reasonable for them to seek a wiretap. Case after case has held that a wiretap may be utilized to determine the contours and dimensions of an otherwise impenetrable conspiracy, where investigators have made diligent but unsuccessful efforts to do so using traditional methods. *E.g., United States v. De La Cruz Suarez*, 601 F.3d 1202, 1214 (11th Cir. 2010) (upholding wiretap where investigators had already uncovered substantial evidence using

pen registers, physical surveillance, and five confidential informants; as further surveillance would increase the likelihood of discovery and searches would tip off coconspirators, agents could use wiretaps to “determine the scope of the conspiracy and all of its members”); *United States v. Johnson*, 393 F. App’x 240, 242 (5th Cir. 2010) (agents may use a wiretap to uncover the scope of a conspiracy when “the affidavit gave specific reasons why physical surveillance, trash pulls, and the use of cameras would risk compromising the investigation because of the geographic layout of the area and would be unlikely to provide information about the scope of the operation or [defendant]’s supplier” and further confidential source purchases posed dangers and “would not likely produce information about other members of the operation or [defendant]’s source”); *United States v. Armenta*, 373 F. App’x 685, 688-89 (9th Cir. 2010) (same); *United States v. Carter*, 449 F.3d 1287, 1293 (D.C. Cir. 2006) (same); *United States v. Jackson*, 345 F.3d 638, 644-45 (8th Cir. 2003) (same); *United States v. Olmedo*, 552 F. Supp. 2d 1347, 1365 (S.D. Fla. 2008) (“where conventional techniques will not show the entire scope of the conspiracy, a wiretap is permissible, even in those situations where conventional techniques will allow for the arrest and

conviction of some members"). The issuing judge had a sound basis for concluding that the government had shown a sufficient "necessity" for the wiretap.⁸

C. Failure to Comply with 18 U.S.C. § 2518

Next, defendants Chisolm and Crawford claim that the wiretap orders are invalid on their face for failing to specify the persons whose communications may be intercepted under 18 U.S.C. § 2518(4)(a), failing to provide a "sufficiently particular description of the type of communication sought to be intercepted" in violation of 18 U.S.C. § 2518(1)(b)(ii) and 18 U.S.C. § 2518(4)(c), and for generally failing to comply with § 2518(4). Doc. 217 at 8-9, 13. These claims amount to little more than a makeweight.

⁸ Bryant's adopted brief makes much of a Second Circuit case, *United States v. Lilla*, 699 F.2d 99 (2d Cir. 1983), but it is distinguishable. In *Lilla*, a police officer had managed a hand-to-hand exchange with a drug dealer but wanted to get a wiretap to nab his cronies. That was the entirety of the investigation. Nevertheless, the officer's wiretap affidavit conclusorily stated that "no other investigative method exists to determine the identity" of individuals involved with the defendant. The *Lilla* court noted that the affidavit was so bad "that the only useful purpose that might be served by the trooper's affidavit . . . is as an exhibit at a police training academy of how not to conform to the federal and state statutory requirements." *Id.* at 105. Unlike the officer in *Lilla*, the agents in this case conducted a lengthy investigation and employed a variety of investigative techniques in an effort to identify and prosecute each member of the conspiracy. Only when those efforts proved unsuccessful did they apply for a wiretap. *Lilla* offers no support for Bryant's argument.

The Court accepts defendants' contention that the wiretap orders, standing alone, were not in strict compliance with the statute. While they did lay out the identity of at least some of those people known by the officers as likely to be intercepted, they did not specify the nature of the communications, the location of the listening posts, or the law enforcement agencies that would be monitoring the wiretaps. Gov't ex. 1, wiretap orders TT1-10. Of course, all of that information *was* set forth in the affidavits and applications accompanying the motions. *Id.* Many courts have pointed out that it is analytically inappropriate to separate the application, affidavit, and order when reviewing for compliance under § 2518(4). *E.g., United States v. Traitz*, 871 F.2d 368, 378-79 (3d Cir. 1989); *United States v. Leisure*, 844 F.2d 1347, 1357 (8th Cir. 1988).

More fundamentally, however, "there is no authority in the case law for the proposition that these particular defects in an authorization of electronic surveillance should result in suppression." *United States v. Restrepo*, 1989 WL 4292 at *3 (D. Conn. Jan. 9, 1989); *United States v. Small*, 423 F.3d 1164, 1178 (10th Cir. 2005) (such technical defects do not undermine the purposes of the statute or prejudice the defendant,

hence suppression is unwarranted); *Traitz*, 871 F.2d at 380 (“suppression is not required for facial insufficiency relating the” identification directives of § 2518(4)); *cf. United States v. Gonzalez Perez*, 283 F. App’x 716, 722 (11th Cir. 2008) (suppression is not the proper remedy for failure to identify all those likely to be overheard where that information did not play a central role in the decision to authorize surveillance); *United States v. Easterling*, 554 F.2d 195, 196 (5th Cir. 1977) (same).⁹

Hence, this claim fails.

D. Minimization

Defendants next argue that the agents failed to comply with their duty to “minimize” under 18 U.S.C. § 2518(5). Doc. 217 at 9. The pertinent statute provides, in part, that “[e]very order and extension thereof shall contain a provision that the authorization to intercept shall be executed . . . in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter.” 18 U.S.C. § 2518(5). The statute “does not prohibit the interception of all non-pertinent conversations; rather it requires the

⁹ *Easterling* is binding Eleventh Circuit authority. *See Bonner v. City of Prichard*, 661 F.2d 1206, 1209 (11th Cir. 1981) (en banc) (adopting as binding precedent all decisions of the former Fifth Circuit decided prior to October 1, 1981).

government to conduct the wiretap so as to minimize the interception of such calls.” *United States v. Armocida*, 515 F.2d 29, 42 (3d Cir. 1974). The minimization standard is “reasonableness,” which is to be assessed on a case-by-case basis. *Id.*

Defendants are silent as to how the agents failed to minimize the interception of unrelated calls. Instead, they simply state that “[u]pon information and belief law enforcement agents failed to comply with the minimization requirement of 18 U.S.C. § 2518(5).” Doc. 217 at 9. They offer no factual support for the claim whatsoever, despite having been given open-file discovery, which includes all of the recordings, call logs, and minimization notes made by the agents who conducted the intercepts. Hence, they have not met their burden of going forward with this claim. *See Patton v. United States*, 2010 WL 3191887 at *7 (W.D. Pa. Aug. 11, 2010); *cf. United States v. Edwards*, 69 F.3d 419, 430 (10th Cir. 1995) (denying appellate review where defendant failed to support his minimization issue “with any reasoned argument or citations to the record”). In any event, the government has met its *prima facie* showing of minimization by including the minimization memoranda along with each wiretap, *United States v. Royster*, 2007 WL 4336321 at *14 (M.D.

Ga. Dec. 7, 2007), which include a long and detailed set of instructions explicitly limiting the intercepting agents to listening to conversations of target subjects relating to specific drug-related criminal offenses. *E.g.*, Gov't ex. 1, TT1 "Monitoring Instructions". Defendants have not come back with any evidence showing that these restrictions were not followed. And even if they had, total suppression of the information gained from the wiretaps is not an appropriate remedy.¹⁰

E. Sealing

Next, defendants claim that the wiretaps were not sealed in accordance with 18 U.S.C. § 2518(8)(a). Doc. 217 at 10. That provision requires that, "[i]mmediately upon the expiration of the period of the

¹⁰ Absent a *flagrant* violation of the minimization requirements, total suppression of all monitored calls is highly unlikely and, quite probably, inappropriate. *See United States v. Ozar*, 50 F.3d 1440, 1448 (8th Cir. 1995) ("Clearly Congress did not intend that evidence directly within the ambit of a lawful order should be suppressed because the officers, while awaiting the incriminating evidence, also gathered extraneous conversations. The non-incriminating evidence could be suppressed pursuant to 18 U.S.C. § 2518(10)(a), but the conversations the warrant contemplated overhearing would be admitted.") (citation omitted); *United States v. Suggs*, 531 F. Supp. 2d 13, 24 (D.D.C. 2008) ("[t]otal suppression 'is not appropriate unless the moving party shows that there was a taint upon the investigation as a whole sufficient to warrant sweeping relief' . . . and is reserved for the 'particularly horrendous case' . . . 'where the government has made effectively no effort towards minimization whatsoever' ") (citations omitted); *United States v. Batiste*, 2007 WL 2412837, at *16 (S.D. Fla. Aug. 21, 2007) (errors in minimizing particular calls do not automatically warrant suppression of all intercepts "unless a defendant demonstrates that the entire surveillance was tainted").

order [authorizing the interception of wire, oral, or electronic communications], or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions." 18 U.S.C. § 2518(8)(a). As a prerequisite to offering testimony concerning the content of the intercepted communications or evidence derived therefrom, the government must show "[t]he presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof. . . ." *Id.* (cross-referencing 18 U.S.C.A. § 2517(3)).

A recording is sealed in accordance with the immediacy requirement of § 2518(8)(a) if it is sealed within one or two days of the expiration of the period of the order. *United States v. Matthews*, 431 F.3d 1296, 1307 (11th Cir. 2005). It is well settled that weekends need not be counted in determining whether sealing orders were filed immediately on the wiretap's expiration. *United States v. Wong*, 40 F.3d 1347, 1375 (2d Cir. 1994); *United States v. Maxwell*, 25 F.3d 1389, 1394 (8th Cir. 1994); *United States v. Carson*, 969 F.2d 1480, 1498 (3d Cir. 1992); *United States v. Rice*, 2005 WL 2180019 at *1 (W.D. Ky. Sep. 9, 2005); *United States v. Bennett*, 825 F. Supp. 1512, 1527 (D. Colo. 1993).

The government's unrebutted recitation shows that all the recordings were timely sealed, save three: TT 4 was four days late, TT 5 was six, and TT 6 was three.¹¹ Doc. 250 at 18. In each instance, the delay resulted from the unavailability of the issuing judge. *Id.* at 18-19. Courts have regularly forgiven delays based on the judge's unavailability absent any tampering with the recordings or prejudice caused to the defendants. *United States v. Kusek*, 844 F.2d 942, 946 (2d Cir. 1988); *United States v. Ardito*, 782 F.2d 358, 363 (2d Cir. 1986); *cf. United States v. Suarez*, 906 F.2d 977, 982 (4th Cir. 1990) (emphasizing that absent prejudice to the defendants or some tactical advantage to the government, courts will generally forgive late sealing). Moreover, courts have forgiven much longer delays with some frequency. *See e.g., United States v. Pedroni*, 958 F.2d 262, 264 (9th Cir. 1992) (forgiving 14-day delay). Here, the delay was relatively short and there is no evidence suggesting bad faith on the government's part or any prejudice to the defendants. Hence, this claim fails.

¹¹ Another record was not sealed for over a month, but no calls had been intercepted on that wiretap. Doc. 250 at 19.

F. Geolocation Data

Defendants argue that the government illegally seized geolocation data in violation of *United States v. Jones*, ___ U.S. ___, 132 S. Ct. 945 (2011). There, the Supreme Court held that the use of a Global Positioning System (“GPS”) tracking device to monitor a vehicle’s movements was a search within the meaning of the Fourth Amendment. That case is inapposite in several respects. First, the affidavits here clearly lay out sufficient probable cause to satisfy the Fourth Amendment’s strictures as to each targeted telephone. Second, even if the wiretap order was too broad in extending to geolocation data from *any* caller who connected to the targeted telephones, defendants have not come forward with facts suggesting that such an interception actually occurred, that the person who was intercepted had standing to raise the issue, or, more fundamentally, that suppression of the entire wiretap is an appropriate remedy for such overbroad language. As the government asserts, “the argument is too general” to warrant serious consideration. Doc. 250 at 20.

III. CONCLUSION

For the above stated reasons, defendants' motions to suppress should be **DENIED**.

SO REPORTED AND RECOMMENDED this 13th day of June, 2013.



UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF GEORGIA